UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

EMC CORPORATION, EMC INFORMATION SYSTEMS INTERNATIONAL, and DELL (CHINA) COMPANY LIMITED,	:	
Plaintiffs,	:	Civil Action No. _____
v.	:	**JURY TRIAL DEMANDED**
XIAOFEI SHAWN SHI,	:	
Defendant.		

COMPLAINT

Plaintiffs EMC Corporation ("Dell EMC"[1]), EMC Information Systems International ("EISI"), and Dell (China) Company Limited ("Dell China"), by and through their undersigned counsel, bring this action against Xiaofei "Shawn" Shi and allege upon knowledge with respect to themselves and their own acts and otherwise upon information and belief with respect to all other matters as follows:

NATURE OF THE ACTION

1. Dell EMC is a wholly-owned subsidiary of Dell Inc. (together with its affiliates, including Dell EMC, EISI, and Dell China[2], "Dell"). Between December 2013 and July 9, 2020, Defendant Shi was employed by Dell in Beijing as a service manager.

[1] EMC Corporation and certain of its affiliates sell products branded as "Dell EMC." This Complaint uses "Dell EMC" to refer solely to EMC Corporation.

[2] Dell China and EISI are indirect subsidiaries of Dell Inc.

2. Among other things, Dell EMC develops, manufactures, and sells enterprise storage array hardware and associated software. These arrays allow businesses to store large amounts of data on multiple physical hard-disk or solid-state drives managed by a central management system.

3. When a customer purchases a Dell EMC array, it purchases not only the array itself and the associated software, but also maintenance services. When Dell EMC performs maintenance on an array, it utilizes a Dell EMC confidential and proprietary diagnostic tool known as SymmWin.

4. SymmWin incorporates numerous Dell EMC trade secrets. For example, SymmWin incorporates technical and engineering information such as: (i) the code constituting SymmWin itself; (ii) compilations of information explaining the various codes and shorthand used to indicate potential problems necessitating servicing; (iii) processes and procedures for diagnosing potential problems necessitating servicing; and (iv) methodologies for diagnosing potential problems necessitating service (the "SymmWin Trade Secrets").

5. Dell EMC personnel or their agents use specifically-authorized and generated credentials to access SymmWin. Those credentials permit Dell EMC to access SymmWin on a particular array and are valid only for a limited (short) amount of time.

6. Barely a year into his employment, Shi sensed an opportunity to enrich himself in connection with the maintenance of certain popular older models of arrays. Exploiting his employment, on information and belief, Shi gained access to Dell EMC's highly confidential technical information — information that he was not authorized to view for his job responsibilities — to learn how to bypass the need for legitimate

credentials to access SymmWin. Armed with this information and his knowledge of Dell EMC's pricing structures for maintenance services gained through his customer service duties, Shi developed *two* side businesses to directly compete with Dell EMC for maintenance services.

7. Shi first created his own companies — Storage Services and StorTec — that compete with Dell EMC to offer third-party maintenance services on Dell EMC arrays. To allow these companies to service Dell EMC products, Shi and those he hired to assist him created a software program that, when installed on an array, bypasses SymmWin's secure authentication mechanism. In this way, Shi gained unfettered and unauthorized access to SymmWin — proprietary Dell EMC software — for his own personal gain.

8. Shi's workaround, though, was not just a necessary tool for Storage Services' and StorTec's servicing business: it also became a second source of illicit revenue to Shi. Beginning in approximately 2016, Shi began selling copies of his software program to *other* third-parties. Shi thus created a shadow network of third-party servicers, all using his software to gain unauthorized access to SymmWin and unfairly compete with Dell EMC for service revenue.

9. Shi's scheme continued unbeknownst to Dell until March 2020, when Dell was alerted to the existence of Shi's software program by an array owner whose service provider had utilized it in providing maintenance. Dell promptly commenced an investigation of the program. Among other things, the investigation revealed Shi to be the mastermind behind the program.

10. Having learned the basics of Shi's scheme through that investigation, Dell scheduled a meeting with Shi on July 9, 2020.

11. After receiving notice of the scheduled meeting, Shi spent the next three days attempting to cover his tracks. Dell IT detected that, on July 6, 7, and 8, 2020, Shi deleted thousands of files from his company-issued laptop, including files explicitly referencing StorTec and Shi's software in their titles, having moved these files to USB storage devices (*i.e.*, external thumb drives and hard drives).

12. During this same time period, Shi blatantly downloaded and absconded with additional files stored on Dell EMC's secure servers in Hopkinton, Massachusetts. These files contain myriad Dell EMC trade secrets related to *all* of Dell EMC's storage devices and describe technical processes, designs, and methodologies for providing maintenance. The bulk of the files stolen by Shi largely were taken from a proprietary application called SolVe Desktop and incorporate Dell EMC trade secrets. For example, the files stolen by Shi include articles, documents, and other items describing scientific, technical, and engineering designs, formulas, code, processes, procedures, methodologies, techniques, and plans relating to the operations, maintenance, and servicing of all Dell EMC storage devices (the "Stolen File Trade Secrets").

13. During the July 9, 2020 meeting, Shi refused to acknowledge his misdeeds or provide any assurances that he would discontinue his illicit businesses. Shi was terminated by Dell at the conclusion of the meeting.

14. As described more fully below, Dell EMC, EISI, and Dell China have suffered damages as a direct and proximate result of the violations of law by Shi and will

continue to suffer irreparable harm as a direct and proximate result of such violations for which there is no adequate remedy at law.

PARTIES

15. Plaintiff Dell EMC is a corporation duly organized and existing under the laws of the Commonwealth of Massachusetts with its principal place of business in Hopkinton, Massachusetts. Dell EMC is the owner of the SymmWin Trade Secrets and Stolen File Trade Secrets, defined herein.

16. Plaintiff EISI is a public unlimited company organized and existing under the laws of the Republic of Ireland with its principal place of business in the Republic of Ireland. Plaintiff EISI is the exclusive licensee outside of the United States of the intellectual property relevant to this action.

17. Plaintiff Dell China is a limited liability company organized and existing under the laws of the People's Republic of China with its principal place of business in the People's Republic of China.

18. On information and belief, Defendant Shi is a citizen and resident of the People's Republic of China. Until July 9, 2020, Defendant Shi was employed by Dell in Beijing as Manager 2, Field Service.

JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this is a civil action arising under 18 U.S.C. § 1836(c) and 18 U.S.C. § 1030. The Court has supplemental jurisdiction over claims arising under the laws of the Commonwealth of Massachusetts pursuant to 28 U.S.C. § 1367(a) because Dell EMC's, EISI's, and Dell China's state law claims are so related to the claims within the Court's

original jurisdiction that they form part of the same case or controversy under Article 3 of the United States Constitution.

20. Defendant Shi is subject to personal jurisdiction pursuant to M.G.L. c. 223A §§3(a) and 3(d) because, as set forth below, Defendant Shi caused injury in the Commonwealth by an act occurring outside the Commonwealth through his transaction of business in the Commonwealth, his solicitation of business in the Commonwealth, his unauthorized accessing of trade secrets stored in the Commonwealth, and his derivation of substantial revenue from goods consumed and services rendered in the Commonwealth.

21. Venue in this district is appropriate pursuant to 28 U.S.C. § 1391(b)(3).

FACTUAL BACKGROUND

22. Dell develops, delivers, and supports information infrastructure and virtual infrastructure technologies, solutions, and services for a broad range of customers, including businesses, governments, not-for-profits, and service providers, around the world and in every major industry, in both public and private sectors, and of sizes ranging from the Fortune 500 to small businesses and individual consumers.

23. Dell EMC's core offerings include hardware and software storage devices, cloud computing, and infrastructure management products, services, and solutions. To that end, and among other things, Dell EMC develops, manufactures, and sells enterprise storage array hardware and associated software that allow businesses to store large amounts of data on multiple physical hard-disk or solid-state drives managed by a central management system.

24. Shi was hired by a Dell EMC affiliate in 2013 as a service manager. During his tenure, Shi was responsible for himself providing, and for overseeing a team that provided, certain servicing functions for customers after their purchase of a Dell EMC storage product, such as installation, configuration, and integration of the product at the customer site, as well as maintenance, troubleshooting, and repair. In this capacity, Shi had access to confidential and proprietary Dell EMC information, including the Stolen File Trade Secrets and information regarding customer lists and arrangements/pricing for maintenance services. In April 2020, after the 2016 acquisition of EMC Corporation by Dell Inc., Shi's employment was transferred to Dell China.

25. Shi signed a Key Employee Agreement ("KEA") with Dell EMC. Under the KEA, Shi was obligated to, among other things: (i) devote his full time and efforts to his employment and not to compete with the company on the side; (ii) keep confidential and protect from disclosure the company's confidential and proprietary business information, including but not limited to its trade secrets and other intellectual property; and (iii) upon his separation from the company, return all documents and other items containing confidential and proprietary business information, including but not limited to documents, programs, or other materials describing or containing trade secrets and other intellectual property. Shi also agreed that his breach of the KEA will cause irreparable harm to Dell EMC. The KEA covered confidential and proprietary information belonging to or obtained through Dell EMC and its affiliates. When Shi's employment was transferred to Dell China, his KEA with Dell EMC remained in place. Additionally, his employment agreements with Dell China contained confidentiality provisions

requiring Shi to keep any business information belonging to Dell confidential and not to disclose or use it for any purpose other than carrying out his job responsibilities.

26. Dell provides products and services to customers in all fifty states and in dozens of countries. To support its interstate and international commercial operations, Dell maintains an interstate and international computer network to which Shi's laptop in Beijing was connected. Of particular note, Dell EMC stores data and files on servers located in and around, among other places, Hopkinton, Massachusetts. All of these computers and servers are connected to the internet, as well as to Dell's network, connecting them directly to one another. Accordingly, through his company-issued laptop physically located in Beijing, Shi was connected to and could access Dell EMC's servers in Hopkinton, which store Dell EMC files and data, including the Stolen Files (defined below).

27. When a customer purchases a Dell EMC storage array, it purchases both: (i) the array's hardware and software; and (ii) maintenance services. As to the latter, while the arrangements vary, upon purchase, a customer typically enters into a service contract for Dell EMC to provide maintenance on the array for one to three years. Dell EMC also offers continued maintenance services after the expiration of the initial contract.

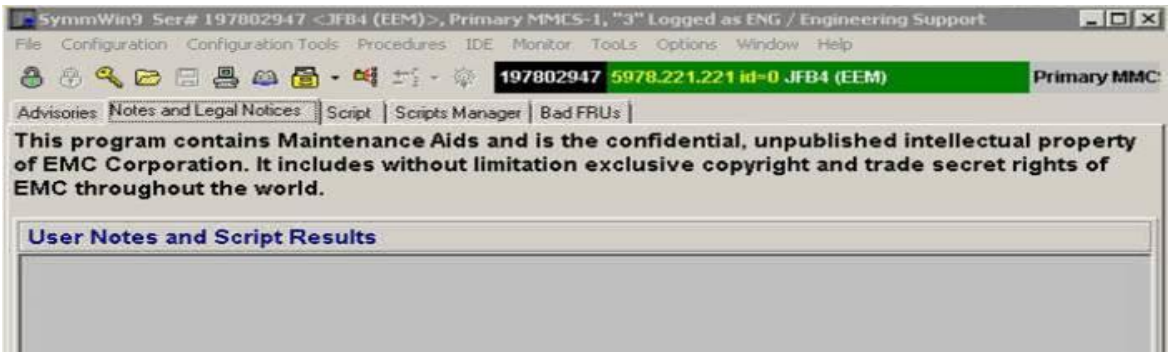
28. To perform maintenance, Dell EMC utilizes software called SymmWin, which is a proprietary program developed through the investment of time, money, and other resources by Dell EMC. SymmWin incorporates the SymmWin Trade Secrets, which include: (i) the code and architectural details constituting SymmWin itself; (ii) compilations of information explaining the various codes and shorthand used to indicate

potential problems necessitating servicing; (iii) processes and procedures for diagnosing potential problems necessitating servicing; and (iv) methodologies for diagnosing potential problems necessitating service.

29. Dell EMC does not grant access to SymmWin to anyone other than its own employees and agents, all of whom are subject to contractual confidentiality provisions as part of their employment or contracts with Dell EMC. Further, the source code and internal architectural details of SymmWin are available only to a small group of Dell engineers who work on the programs and who are also subject to contractual confidentiality obligations as part of their employment.

30. Additionally, access to SymmWin is gated by a secure authentication system. To access SymmWin, authorized Dell EMC personnel and agents must enter a valid set of credentials. Credentials are generated by Dell EMC using the serial number of the array to which the user requires access. Accordingly, the credentials can be used only on the specific array for which they are generated. Each set of credentials is valid for a specific amount of time, typically one to two days (with an outer limit of ten days). When the credentials expire, Dell EMC must generate new credentials, with a new expiration date, for the user to continue accessing SymmWin.

31. Dell EMC explicitly marks SymmWin as confidential and proprietary. At each stage of the log-in and authentication process, banners and other messages inform the user in bold lettering that access to SymmWin is restricted and that SymmWin is a confidential and proprietary Dell EMC program:



32. SymmWin and the SymmWin Trade Secrets are economically valuable to Dell EMC. SymmWin and the SymmWin Trade Secrets enable Dell EMC to provide maintenance services on its customers' storage arrays in exchange for a fee.

33. Shi exploited his employment to access confidential information, including the SymmWin Trade Secrets, to learn how to engineer access to SymmWin without proper credentials. Having done so, while employed by Dell and using his Dell-issued laptop and other Dell supplies, Shi then started not one, but two side businesses to enrich himself at the expense of Dell EMC. Shi's businesses are directly dependent on his covert and unauthorized use of trade secret and other confidential and proprietary information belonging to Dell EMC and directly compete with Dell EMC on the back of that information.

34. Shi's first business provides maintenance services to array owners whose initial service contracts have expired. Through two entities he formed in China — StorTec and Storage Services — Shi offers unauthorized third-party maintenance to Chinese customers in direct competition with Dell EMC. Shi does this by utilizing software he created or caused to be created that incorporates misappropriated SymmWin Trade Secrets, among other confidential and proprietary information, to bypass SymmWin's authentication mechanism.

35. Shi and his companies also began to sell access to Shi's illicit access software to other third-party servicers all over the world. One of Shi's frequent customers has been the Framingham-based GloboParts, Inc. and its principal, Eric Hukki. Shi has contacted Hukki in the Commonwealth since at least 2017 and appears to have sold numerous copies of his software to GloboParts and/or Hukki. On information and belief, GloboParts and/or Hukki have used this software to service Dell EMC arrays located in the Commonwealth.

36. Among other things, because of the KEA and the various steps Dell EMC takes to protect the SymmWin Trade Secrets, Shi knew or had reason to know that his access to and use of the SymmWin Trade Secrets to develop his software and compete with Dell EMC exceeded the scope of his authorized access to the SymmWin Trade Secrets.

37. Dell EMC has lost maintenance service revenue as a direct result of Shi's actions to unfairly compete and to sell his software so that others may unfairly compete for maintenance services. Based on the number of copies of his software that it believes through its investigation that Shi either used himself or sold to third parties (and the number of affected arrays), Dell EMC estimates that its lost servicing revenue is in the millions of dollars.

38. On or about March 2020, when the owner of an array in Europe reached out for assistance with a maintenance issue related to Shi's software, Dell began to uncover Shi's disloyal and illicit side businesses.

39. Dell conducted an investigation that ultimately led to the collection of extensive evidence of Shi's guilt. Dell scheduled a meeting with Shi in July 2020 to confront him with the evidence it had collected.

40. Upon receiving notice of the scheduled meeting, Shi, likely sensing that his illegal activities had been uncovered, immediately began trying to erase the evidence of his wrongdoing. Over the course of the next three days, Shi deleted thousands of files from his company-issued laptop regarding his improper activities. These files included documents and folders explicitly referencing StorTec and the name of his software. While deleting the files from his company-issued computer, he copied them to external storage devices.

41. In the midst of his deletion spree, Shi also accessed, downloaded, and copied hundreds of proprietary and confidential documents from Dell servers onto his company laptop and then onto several external media devices (the "Stolen Files"). Most of the Stolen Files are stored on Dell EMC's servers in Hopkinton, Massachusetts. To download them, Shi was required to access those Massachusetts-based servers through the internet-connected networks linking Dell's computers in China — including Shi's laptop — with the servers in Hopkinton, which are used in interstate and foreign commerce, including but not limited to in the manner described below.

42. In particular, Shi accessed, downloaded, and copied hundreds of files from a Dell EMC database called SolVe Desktop ("SolVe"). SolVe houses proprietary and confidential information that Dell field service engineers use to conduct maintenance on customer storage devices. SolVe contains information on all Dell EMC high-end storage products, including but not limited to the models of Dell EMC arrays that were targeted

by Shi in his scheme. SolVe also contains some information from Dell EMC and its agents related to servicing activities they have performed on Dell EMC arrays throughout the world.

43. Specifically, SolVe contains videos and other internal knowledge-based articles and other materials associated with Dell storage products, including lengthy "white papers" that describe in detail information needed to service the products. The "white papers" and the other information on SolVe contain confidential and proprietary information developed by Dell EMC through years of experience and further development of technical know-how, scientific, technical, and engineering designs, formulas, processes, procedures, methodologies, techniques, plans, and code relating to the operations, maintenance, and servicing of Dell EMC storage devices — the Stolen File Trade Secrets. Dell EMC is the owner of the Stolen File Trade Secrets, having developed most of them prior to its acquisition by Dell Inc.

44. As its contents are confidential, proprietary, and competitively valuable, the public cannot access SolVe. Accordingly, when a user logs into SolVe, much like with SymmWin, banners and other messages inform the user in bold lettering that access to SolVe is restricted and that SolVe is a confidential and proprietary program.

45. Access to SolVe is limited to certain individuals within three increasingly broad tiers of access: Customers, Partners, and Employee. Customer and Partner access requires that the customer or partner agree to confidentiality provisions. With respect to Employee access, only certain Dell EMC employees have access to SolVe. Dell EMC does *not* grant SolVe access to all employees; access is given only to those employees who might need to reference SolVe as part of their job duties. Even employees with

access to SolVe do not have unfettered access: they must request access when it is needed, and access is granted for a 14-day period. Reauthentication — including through the use of new credentials generated by Dell — is required after that 14-day period.

46. Dell EMC derives significant economic benefit from SolVe. Access to the Customer level of SolVe is part of the purchase price of the product, access to the Partner level of SolVe is through a licensing fee, and Dell EMC utilizes SolVe to sell maintenance services to owners of Dell EMC storage products. The Stolen Files are therefore also valuable to Shi, who can now use them to compete with Dell to provide maintenance services through StorTec and Storage Services.

47. Dell EMC spent many years and significant sums creating SolVe, developing the maintenance solutions described therein, and perfecting those maintenance solutions.

48. Shi knew or had reason to know that his access, downloading, and copying of the Stolen Files exceeded the scope of his authorized access. During the course of his employment, upon request (*see* ¶ 45), Shi could obtain access to SolVe. However, Shi's access to SolVe (and other Dell EMC proprietary materials) was not unlimited. As Shi was aware, Shi was required to access SolVe materials only on an as-needed basis to fulfill a legitimate business purpose. Under no circumstances was Shi permitted to access, download, or copy SolVe files — much less hundreds of them — for his personal use or the use of his (illicit) side businesses competing with Dell EMC. Stated differently, regardless of the fact that he was granted access to SolVe as an employee for the purpose of carrying out his responsibilities *for Dell*, Shi was not authorized to access

SolVe for purposes *adverse to Dell*, including competing with Dell EMC by misappropriating its confidential and proprietary information.

49. Shi's intrusion into Dell EMC's Hopkinton servers to access and download the Stolen Files from SolVe caused damage to Dell EMC. Not only are the files themselves independently economically valuable, used by Dell EMC to offer maintenance services to customers, but Dell was forced to hire a forensic investigator to assess the scope of Shi's intrusion. The amount of this engagement exceeds $5,000.

COUNT ONE
(Violation of Defend Trade Secrets Act, 18 U.S.C. § 1836)

50. Dell EMC and EISI restate and incorporate by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

51. Dell EMC is the owner of the Stolen Files, which are and contain significant confidential business information, including but not limited to the Stolen File Trade Secrets. EISI is the exclusive licensee outside of the United States of the trade secrets relating to and embodied in the Stolen Files.

52. The Stolen File Trade Secrets constitute valid and enforceable trade secrets.

53. The Stolen File Trade Secrets are confidential, proprietary, and economically valuable. The Stolen File Trade Secrets are not generally known or readily ascertainable. Dell EMC took reasonable precautions to maintain the secrecy of the Stolen File Trade Secrets, including confidentiality provisions in key employment agreements and separate confidentiality agreements with employees, the use of credentials needed to access the Stolen Files, and limitation of access of the Stolen Files

only to certain employees and authorized third parties (which third parties are subject to confidentiality agreements).

54. Shi acquired the Stolen File Trade Secrets by improper means. Specifically, Shi exceeded the scope of his authorized access — granted to him by virtue of his employment — to unlawfully download and remove the Stolen Files for purposes other than fulfilling his job responsibilities. Shi knew or had reason to know that his acquisition of the Stolen File Trade Secrets was through improper means.

55. On information and belief, Shi also used or will use the Stolen Files in connection with his illicit businesses.

56. Dell EMC and EISI have suffered damages in an amount to be proven at trial as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT TWO
(Violation of Defend Trade Secrets Act, 18 U.S.C. § 1836)

57. Dell EMC and EISI restate and incorporate by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

58. Dell EMC is the owner of the SymmWin Trade Secrets, which constitute valid and enforceable trade secrets. EISI is the exclusive licensee outside of the United States of the SymmWin Trade Secrets.

59. The SymmWin Trade Secrets are confidential, proprietary, and economically valuable. The SymmWin Trade Secrets are not generally known or readily ascertainable. Dell EMC took reasonable precautions to maintain the secrecy of the SymmWin Trade Secrets, including confidentiality provisions in key employment

agreements and separate confidentiality agreements with employees, the use of secure credentials needed to access the SymmWin Trade Secrets, and limitation of access of the SymmWin Trade Secrets only to certain employees.

60. Shi acquired the SymmWin Trade Secrets by improper means. Specifically, Shi exceeded the scope of his authorized access — granted to him by virtue of his employment — to unlawfully access, view, and copy the SymmWin Trade Secrets for purposes other than fulfilling his job responsibilities.

61. Shi also improperly used the SymmWin Trade Secrets by creating, using, and/or selling his illicit software. Shi knew or had reason to know that he had acquired access to the SymmWin Trade Secrets by improper means. Even if Shi had acquired the SymmWin Trade Secrets through proper means (he did not), Shi was under a duty pursuant to the KEA to refrain from using Dell EMC's trade secrets for any purpose other an execution of his job duties.

62. Dell EMC and EISI have suffered damages in an amount to be proven at trial as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT THREE
(Violation of Massachusetts Uniform Trade Secrets Act, M.G.L. c. 93, § 42)

63. Dell EMC and EISI restate and incorporate by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

64. Dell EMC is the owner of the Stolen Files, which are and contain significant confidential business information, including but not limited to the Stolen File

Trade Secrets. EISI is the exclusive licensee outside of the United States of the trade secrets relating to and embodied in the Stolen Files.

65. The Stolen File Trade Secrets constitute valid and enforceable trade secrets.

66. The Stolen File Trade Secrets are confidential, proprietary, and economically valuable. The Stolen File Trade Secrets are not generally known or readily ascertainable. Dell EMC took reasonable precautions to maintain the secrecy of the Stolen File Trade Secrets, including confidentiality provisions in key employment agreements and separate confidentiality agreements with employees, the use of secure credentials needed to access the Stolen Files, and limitation of access of the Stolen Files only to certain employees and authorized third parties (which third parties are subject to confidentiality agreements).

67. Shi acquired the Stolen File Trade Secrets by improper means. Specifically, Shi exceeded the scope of his authorized access — granted to him by virtue of his employment — to unlawfully download and remove the Stolen Files for purposes other than fulfilling his job responsibilities. Shi knew or had reason to know that his acquisition of the Stolen File Trade Secrets was through improper means.

68. On information and belief, Shi also used or will use the Stolen Files in connection with his illicit businesses.

69. Dell EMC and EISI have suffered damages in an amount to be proven at trial as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT FOUR
(Violation of Massachusetts Uniform Trade Secrets Act, M.G.L. c. 93, § 42)

70. Dell EMC and EISI restate and incorporate by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

71. Dell EMC is the owner of the SymmWin Trade Secrets, which constitute valid and enforceable trade secrets. EISI is the exclusive licensee outside of the United States of the SymmWin Trade Secrets.

72. The SymmWin Trade Secrets are confidential, proprietary, and economically valuable. The SymmWin Trade Secrets are not generally known or readily ascertainable. Dell EMC took reasonable precautions to maintain the secrecy of the SymmWin Trade Secrets, including confidentiality provisions in key employment agreements and separate confidentiality agreements with employees, the use of secure credentials needed to access the Stolen Files, and limitation of access of the SymmWin Trade Secrets only to certain employees.

73. Shi acquired the SymmWin Trade Secrets by improper means. Specifically, Shi exceeded the scope of his authorized access — granted to him by virtue of his employment — to unlawfully access, view, and copy the SymmWin Trade Secrets for purposes other than fulfilling his job responsibilities.

74. Shi also improperly used the SymmWin Trade Secrets by creating, using, and/or selling his illicit software. Shi knew or had reason to know that he had acquired access to the SymmWin Trade Secrets by improper means. Even if Shi had acquired the SymmWin Trade Secrets through proper means (he did not), Shi was under a duty pursuant to the KEA to refrain from using Dell EMC's trade secrets for any purpose other an execution of his job duties.

75. Dell EMC and EISI have suffered damages in an amount to be proven at trial as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT FIVE
(Misappropriation of Confidential Business Information)

76. Dell EMC and EISI restate and incorporate by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

77. Dell EMC's business relies upon confidential and proprietary business information, including but not limited to the SymmWin Trade Secrets and the Stolen File Trade Secrets. EISI is the exclusive licensee of the trade secrets relating to and embodied in the Stolen Files and the SymmWin Trade Secrets. Even if not amounting to trade secrets, the Stolen File Trade Secrets and SymmWin Trade Secrets are confidential and proprietary business information.

78. The Stolen File Trade Secrets and SymmWin Trade Secrets are confidential, proprietary, and economically valuable. They are not generally known or readily ascertainable. Dell EMC took reasonable precautions to maintain their secrecy, including confidentiality provisions in key employment agreements and separate confidentiality agreements with employees, the use of secured, password-protected networks and databases, the use of secured, Dell EMC-generated credentials necessary to access the Stolen Files and the SymmWin Trade Secrets, and confidentiality agreements with any third parties to whom any confidential business information is disclosed.

79. Shi acquired the Stolen Files and the SymmWin Trade Secrets by improper means. Specifically, Shi exceeded the scope of his authorized access —

granted to him by virtue of his employment — to unlawfully access, view, and copy the Stolen Files and the SymmWin Trade Secrets for purposes other than fulfilling his job responsibilities.

80. Shi also improperly used the SymmWin Trade Secrets by creating, using, and/or selling his illicit software. Shi knew or had reason to know that he had acquired access to the SymmWin Trade Secrets by improper means. Even if Shi had acquired the SymmWin Trade Secrets through proper means (he did not), Shi was under a duty pursuant to the KEA to refrain from using Dell EMC's trade secrets for any purpose other an execution of his job duties.

81. On information and belief, Shi also used or will use the Stolen Files in connection with his illicit businesses.

82. Dell EMC and EISI have suffered damages in an amount to be proven at trial as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT SIX
(Conversion)

83. Dell EMC restates and incorporates by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

84. Dell EMC owns the Stolen Files. Shi, having ended his employment, has no right to exercise dominion or control over the Stolen Files or the SymmWin Trade Secrets absent Dell EMC's consent. Shi likewise has no right, absent Dell EMC's consent, to use the Stolen Files or the SymmWin Trade Secrets in a manner that deprives Dell EMC of its ownership interest in the Stolen Files. Even while employed, Shi had no

right to exercise dominion or control over the Stolen Files or the SymmWin Trade Secrets — his access to the Stolen Files and the SymmWin Trade Secrets exceeded his authorized access. Likewise, even while employed, Shi had no right to use the Stolen Files or the SymmWin Trade Secrets in a matter that deprived Dell EMC of its ownership interest in the Stolen Files and the SymmWin Trade Secrets.

85. By his actions, Shi has deprived Dell EMC of the actual and beneficial ownership of the Stolen Files and the SymmWin Trade Secrets.

86. Dell EMC has suffered damages as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT SEVEN
(Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

87. Dell EMC restates and incorporates by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

88. Dell EMC's computers, servers, and network, including but not limited to its servers in Hopkinton, Massachusetts are protected computers. Dell EMC's computers, servers, and network are used in and affect interstate and foreign commerce and communications.

89. To fulfill his job duties, Shi was authorized to access certain of the Stolen Files upon request of credentials for a proper business purpose. Shi exceeded his authorization, however, by intentionally accessing, downloading, and copying the Stolen Files for his personal use, the use of his companies, or for the use of any other third parties, in order to further his or their interests. Shi intentionally exceeded his

authorization by accessing, downloading, and copying the Stolen Files for purposes adverse to Dell EMC's interests.

90. Through his access in excess of his authority, Shi obtained data from Dell EMC's protected computers. Shi intentionally downloaded, copied, and removed from Dell EMC hundreds of Stolen Files.

91. Dell EMC has suffered losses in an amount exceeding $5,000. Among other things, on information and belief, Shi also used or will use the Stolen Files in connection with his illicit businesses.

92. Dell EMC has suffered damages as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT EIGHT
(Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

93. Dell EMC restates and incorporates by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

94. Dell EMC's computers, servers, and network, including but not limited to its servers in Hopkinton, Massachusetts are protected computers. Dell EMC's computers, servers, and network are used in and affect interstate and foreign commerce and communications.

95. To fulfill his job duties, Shi was authorized to access certain confidential and proprietary Dell EMC information related to the SymmWin Trade Secrets. Shi exceeded his authorized access by obtaining the SymmWin Trade Secrets and using them to create his illicit software, actions all adverse to Dell EMC's interests.

96. Through his unauthorized access and/or access in excess of his authority, Shi obtained data from Dell EMC's protected computers. Shi viewed and used the SymmWin Trade Secrets, or some of them, to incorporate them into his illicit software.

97. Dell EMC has suffered losses in an amount exceeding $5,000.

98. Dell EMC has suffered damages as a direct and proximate result of the violations of law by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations of law for which there is no adequate remedy at law.

COUNT NINE
(Breach of Contract)

99. Dell EMC restates and incorporates by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

100. The KEA is a valid and binding contractual agreement between Dell EMC and Shi.

101. The KEA was made for valid consideration. Under the KEA and other terms of his employment, Shi received the equivalent of hundreds of thousands U.S. dollars of total compensation and access, during his employment, to Dell EMC confidential information.

102. Dell EMC fully performed its obligations under the KEA.

103. Shi breached the KEA by failing to devote his full time and efforts to Dell EMC when he: (i) devoted time and effort to the creation of StorTec, Storage Services, and his illicit software; (ii) devoted time and effort to conducting business through StorTec, Storage Services, and individually; and (iii) devoted time and effort to selling his illicit software to third parties.

104. Shi also breached the KEA by competing with Dell EMC in the market for maintenance services individually and/or through StorTec and/or Storage Services, including but not limited to by using and selling his illicit software.

105. As a direct and proximate result of Shi's breach of the KEA, Dell EMC has suffered damages in an amount to be proven at trial.

106. Dell EMC has suffered and will continue to suffer irreparable harm as a result of Shi's violations of law and contract for which there is no adequate remedy at law, as Shi acknowledged in the KEA.

COUNT TEN
(Breach of Contract)

107. Dell EMC restates and incorporates by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

108. The KEA is a valid and binding contractual agreement between Dell EMC and Shi.

109. The KEA was made for valid consideration. Under the KEA and other terms of his employment, Shi received the equivalent of hundreds of thousands U.S. dollars of total compensation and access, during his employment, to Dell EMC confidential information.

110. Dell EMC fully performed its obligations under the KEA.

111. Shi breached the KEA by using Dell EMC's confidential information for his own benefit and the benefit of his side businesses, including but not limited to the Stolen File Trade Secrets and the SymmWin Trade Secrets.

112. As a direct and proximate result of Shi's breach of the KEA, Dell EMC has suffered damages in an amount to be proven at trial.

113. Dell EMC has suffered and will continue to suffer irreparable harm as a result of Shi's violations of law and contract for which there is no adequate remedy at law, as Shi acknowledged in the KEA.

COUNT ELEVEN
(Breach of Contract)

114. Dell EMC restates and incorporates by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

115. The KEA is a valid and binding contractual agreement between Dell EMC and Shi.

116. The KEA was made for valid consideration. Under the KEA and other terms of his employment, Shi received the equivalent of hundreds of thousands U.S. dollars of total compensation and access, during his employment, to Dell EMC confidential information.

117. Dell EMC fully performed its obligations under the KEA.

118. Shi breached the KEA by failing to return all Dell EMC confidential and proprietary information, materials, documents, and property, including but not limited to the Stolen Files, upon the termination of his employment.

119. As a direct and proximate result of Shi's breach of the KEA, Dell EMC has suffered damages in an amount to be proven at trial.

120. Dell EMC has suffered and will continue to suffer irreparable harm as a result of Shi's violations of law and contract for which there is no adequate remedy at law, as Shi acknowledged in the KEA.

COUNT TWELVE
(Breach of the Duty of Loyalty)

121. Dell EMC and Dell China restate and incorporate by reference all of the allegations contained in the foregoing paragraphs as if fully set forth herein.

122. Shi occupied a position of trust and confidence within Dell EMC and later Dell China. Shi was a manager and had access to significant amounts of confidential information pursuant to his job duties, including in-depth customer information and certain confidential business intellectual property.

123. Accordingly, Shi owed Dell EMC and Dell China a duty of loyalty.

124. Shi breached his duty of loyalty when, for the purpose of furthering his own interests that were adverse to Dell EMC's and Dell China's interests he: (i) diverted his time and efforts to creating StorTec, Storage Services, and his illicit software; (ii) used Dell EMC's resources, trade secrets, other intellectual property, and confidential business information to create his illicit software; (iii) competed with Dell EMC for maintenance business; and (iv) stole files containing trade secrets from Dell EMC.

125. Dell EMC and Dell China have suffered damages as a direct and proximate result of the violations of duty by Shi, and will continue to suffer irreparable harm as a direct and proximate result of such violations for which there is no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Dell EMC, EISI, and Dell China respectfully request that this Court enter judgment in their favor against Shi and award Dell EMC, EISI, and Dell China the following relief:

(a) monetary damages to the extent they may be ascertained and in an amount to be determined at trial, but in no event less than $75,000;

(b) restitution and/or disgorgement of ill-gotten gains;

(c) punitive damages to the extent permitted by law;

(d) reasonable costs and attorneys' fees in prosecution of its claims to the extent permitted by contract or law;

(e) pre-and post-judgment interest;

(f) preliminary and/or permanent equitable relief, including but not limited to a preliminary and permanent injunction enjoining Shi from continuing the acts of unlawful practices set forth above; and

(g) such other relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs Dell EMC, EISI, and Dell China demand a jury trial on all claims so triable.

Dated: August 7, 2020
Boston, Massachusetts

Respectfully submitted,

/s/ *James R. Carroll*

James R. Carroll (BBO #554426)
Marley Ann Brumme (BBO # 687822)
SKADDEN, ARPS, SLATE,
MEAGHER & FLOM LLP
500 Boylston Street
Boston, Massachusetts 02116
(617) 573-4800
james.carroll@skadden.com
marley.brumme@skadden.com

P. Anthony Sammi
SKADDEN, ARPS, SLATE,
MEAGHER & FLOM LLP
One Manhattan West
New York, New York 10001
(212) 735-3000
anthony.sammi@skadden.com

Counsel for Plaintiffs EMC Corporation, EMC Information Systems International, and Dell (China) Company Limited